NSTISSI No. 4013
August 1997

NATIONAL TRAINING STANDARD

FOR

SYSTEM ADMINISTRATORS

IN

INFORMATION SYSTEMS SECURITY

(INFOSEC)

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY

National Security Telecommunications And Information Systems Security Committee

NATIONAL MANAGER

FOREWORD

1. This instruction establishes the minimum course content or standard for the development and implementation of training for system administrator professionals in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this instruction from:

NATIONAL SECURITY AGENCY
NSTISSC SECRETARIAT
ATTN: V503 STE 6716
Fort GEORGE G. MEADE, MD 20755-6716

KENNETH A. MINIHAN
Lieutenant General, USAF

NATIONAL TRAINING STANDARD
FOR
SYSTEM ADMINISTRATORS
IN
INFORMATION SYSTEMS SECURITY (INFOSEC)

SECTION I - PURPOSE

1. This instruction establishes the minimum training standard for the development and implementation of training for System Administrators in the disciplines of telecommunications and information systems (IS) security.

SECTION II - APPLICABILITY

2. National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501 establishes the requirement for federal departments and agencies to implement training programs for INFOSEC professionals. As defined in NSTISSD 501, an INFOSEC professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle. That directive is being implemented in a synergistic environment among departments and agencies which are committed to satisfying these INFOSEC education and training requirements in the most effective and efficient manner possible. This instruction is the continuation of a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (NSTISSI Nos. 4011, 4012, 4013, and 4014). The definitions for words used in this instruction are derived from the National INFOSEC Glossary, NSTISSI No. 4009. The references pertinent to this instruction are listed in ANNEX B. Other documents which can be used in conjunction with this document are listed in ANNEX C.

3. The body of knowledge listed in this instruction may be obtained from a variety of sources, i.e., the National Cryptologic School, the General Services Administration (Office of Information Security), and Government contractors, as well as from adaptations of existing department/agency training programs, or from a combination of experience and formal training. ANNEX A lists the minimal INFOSEC performance standard for an SA.

4. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of training for System Administrators in the disciplines of telecommunications and IS security.

SECTION III - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure that System Administrators (or their equivalents) are made aware of the body of knowledge outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

6. The National Manager shall:

a. maintain and provide an INFOSEC training standard for System Administrators to U.S. Government departments and agencies;

b. ensure that appropriate INFOSEC training courses for System Administrators are developed; and

c. assist other U.S. Government departments and agencies in developing and/or conducting INFOSEC training activities for System Administrators as requested.

ANNEX A

MINIMAL INFOSEC PERFORMANCE STANDARD FOR SYSTEM ADMINISTRATORS

Job functions

The INFOSEC functions of a System Administrator are:

(1) working closely with the Information Systems Security Officer (ISSO) to ensure the Information System or network is used securely;
(2) participating in the Information Systems Security incident reporting program;
(3) assisting the ISSO in maintaining configuration control of the systems and applications software;
(4) advisingthe ISSO of security anomalies or integrity loopholes; and
(5) administering, when applicable, user identification or authentication mechanism(s) of the IS or network.

Terminal Objective:

Given various simulated scenarios and typical situations containing information systems security issues, the System Administrator will be able to describe and apply the appropriate actions to manage and administer the IS(s) in a secure manner. To be acceptable, the description must be in accordance with applicable INFOSEC regulations, policies, and guidelines.

List of performance items under competencies

In each of the competency areas listed below, the System Administrator shall perform the following functions:

1. GENERAL

a. Security Policy

(1) define local accountability policies;
(2) explain accreditation;
(3) discuss three agency specific security policies;
(4) define assurance;
(5) explain certification policies as related to local requirements;
(6) define local e-mail privacy policies;
(7) describe local security policies relative to electronic records management;
(8) explain security policies relating to ethics;
(9) describe relevant FAX security policies;
(10) discuss the concept of information confidentiality;
(11) identify information ownership of data held under his/her cognizance;
(12) identify information resource owner/custodian;
(13) define local information security policy;
(14) describe information sensitivity in relation to local policies;
(15) discuss integrity concepts;
(16) describe local policies relevant to Internet security;
(17) explain local area network (LAN) security as related to local policies;
(18) define policies relating to marking of sensitive information;
(19) understands fundamental concepts of multilevel security;
(20) describe policies relevant to network security;

(21) define the functional requirements for operating system integrity;
(22) perform operations security (OPSEC) in conformance with local policies;
(23) explain physical security policies;
(24) discuss local policies relating to secure systems operations;
(25) identify appropriate security architecture for use in assigned IS(s);
(26) describe security domains as applicable to local policies;
(27) define local policies relating to separation of duties;
(28) identify systems security standards policies;
(29) identify DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), or Orange Book policies;
(30) identify TEMPEST policies;
(31) define TEMPEST policies;
(32) define validation and testing policies;
(33) identify verification and validation process policies;
(34) define verification and validation process policies;
(35) describe wide area network (WAN) security policies;
(36) use/implement WAN security policies;
(37) describe workstation security policies;
(38) use/implement workstation security policies; and
(39) describe zoning and zone of control policies.

b. Procedures

(1) practice/use facility management procedures;
(2) describe FAX security procedures;
(3) practice/use FAX security procedures;
(4) describe housekeeping procedures;
(5) perform housekeeping procedures;
(6) describe information states procedures;
(7) distinguish among information states procedures;
(8) explain Internet security procedures;
(9) use Internet security procedures;
(10) explain marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms, March 30, 1987);
(11) perform marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms, March 30, 1987);
(12) apply multilevel security;
(13) explain the principles of network security procedures;
(14) use network security procedures;
(15) describe operating system integrity procedures;
(16) perform operating systems security procedures;
(17) assist in local security procedures;
(18) describe purpose and contents of National Computer Security Center TG-005, Trusted Network Interpretation (TNI), or Red Book;
(19) describes secure systems operations procedures;
(20) define TEMPEST procedures;
(21) identify TEMPEST procedures;
(22) identify certified TEMPEST technical authority (CTTA);
(23) describe WAN security procedures;
(24) practice WAN security procedures; and
(25) explain zoning and zone of control procedures.

c. Education, Training, and Awareness

(1) discuss the principle elements of security training;
(2) explain security training procedures;
(3) explain threat in its application to education, training, and awareness;
(4) use awareness materials as part of job;
(5) distinguish between education, training, and awareness;
(6) give examples of security awareness;
(7) give examples of security education;
(8) discuss the objectives of security inspections/reviews; and
(9) identify different types of vulnerabilities.

d. Countermeasures/Safeguards

(1) discuss the different levels of countermeasures/safeguards assurance;
(2) describe e-mail privacy countermeasures/safeguards;
(3) define Internet security;
(4) describe what is meant by countermeasures/safeguards;
(5) describe separation of duties;
(6) define countermeasures/safeguards used to prevent software piracy;
(7) define TEMPEST countermeasures/safeguards; and
(8) explain what is meant by zoning and zone of control.

e. Risk Management

(1) explain ways to provide protection for Internet connections;
(2) describe operating system integrity;
(3) define TEMPEST as it relates to the risk management process;
(4) identify different types of threat;
(5) explain WAN security; and
(6) explain what zoning and zone of control ratings are based on.

2. ACCESS CONTROL

a. Policies/Administration

(1) use network access controls as designed;
(2) explain compartmented/partitioned mode;
(3) describe data access;
(4) identify the dedicated mode of operation;
(5) explain electronic records management;
(6) define information ownership;
(7) identify information resource owner/custodian;
(8) describe separation of duties; and
(9) define the system high mode.

b. Countermeasures

(1) describe use of caller ID;
(2) give five examples of countermeasures;
(3) define internal controls and security;
(4) identify methods of intrusion detection;
(5) define network firewalls; and
(6) describe network security software.

c. Safeguards

(1) demonstrate the ability to use alarms, signals, and reports;
(2) identify network security software;
(3) describe operating system security features;
(4) define protected distribution systems; and
(5) describe system security safeguards.

d. Mechanisms

(1) discuss authentication mechanisms;
(2) describe discretionary access controls;
(3) describe mandatory access controls;
(4) describe one-time passwords;
(5) discuss privileges; and
(6) define single sign-on.

3. ADMINISTRATIVE

a. Policies/Procedures

(1) identify basic/generic management issues;
(2) define change control policies;
(3) discuss documentation;
(4) explain electronic records management;
(5) describe object reuse;
(6) define operational procedure review;
(7) discuss policy enforcement;
(8) identify procedures;
(9) discuss security inspections; and
(10) describe local password management policy.

b. Countermeasures/Safeguards

(1) give examples of alarms, signals and reports;
(2) define application development control;
(3) assist in preparing assessments;
(4) identify countermeasures;
(5) describe disaster recovery procedures;
(6) discuss disposition of classified information;
(7) practice disposition of media and data;
(8) practice document labeling;
(9) discuss proper use of security safeguards;
(10) define separation of duties;
(11) identify storage media protection and control; and
(12) define system software controls.

4. AUDIT

a. Policies/Procedures

(1) use alarms, signals and reports in accordance with existing policies and procedures;
(2) summarize audit-related documentation;
(3) discuss electronic records management relative to compliance with local policies and procedures; and
(4) describe three policies and/or procedures in which separation of duties is appropriate or mandatory.

b. Countermeasures/Safeguards

(1) identify two countermeasures applicable to audit trail tampering; and
(2) describe three safeguards gained through use of audit trails.

c. Tools

(1) explain two major benefits of auditing;
(2) identify three audit tools;
(3) describe the major benefit gained through use of audit trails and logging policies;
(4) define an error log;
(5) explain two capabilities offered by expert security/audit tools;
(6) identify two intrusion detection systems; and
(7) describe the major operating system security features.

5. OPERATIONS

a. Policies/Procedures

(1) describe disaster recovery policies and procedures;
(2) use/implement disaster recovery policies and procedures;
(3) define disaster recovery policies and procedures;
(4) describe documentation policy and procedures;
(5) use/implement documentation policy and procedures;
(6) discuss object reuse policy and procedures;
(7) describe separation of duties policies and procedures;
(8) practice/implement separation of duties policies and procedures;
(9) identify disposition of media and data policies and procedures;
(10) perform disposition of media and data policies and procedures;
(11) explain disposition of media and data policies and procedures; and
(12) identify storage media protection/control policies and procedures.

b. Countermeasures/Safeguard

(1) use countermeasure/safeguard alarms, signals and reports;
(2) describe countermeasures;
(3) use/implement countermeasures/safeguards;
(4) discuss countermeasure/safeguard corrective actions;
(5) assist in performing countermeasure/safeguard corrective actions;
(6) describe safeguards; and
(7) use/implement safeguards.

c. Management/Oversight

(1) use/implement management/oversight change controls;
(2) describe configuration management;

(3) discuss database integrity;
(4) describe disaster recovery management/oversight;
(5) use/implement disaster recovery management/oversight;
(6) discuss electronic records management/oversight;
(7) identify the key elements of information integrity;
(8) discuss information management;
(9) explain risk management; and
(10) practice risk management.

6. CONTINGENCY

a. Continuity of Operations

(1) practice backups;
(2) describe continuity planning;
(3) describe disaster recovery;
(4) describe disaster recovery plan testing; and
(5) discuss disaster recovery planning.

b. Countermeasures/Safeguards

(1) use alarms, signals and reports;
(2) define information availability;
(3) identify examples of corrective actions;
(4) select countermeasures;
(5) identify methods of intrusion detection; and
(6) select appropriate safeguards.

c. Configuration Management

(1) practice change controls;
(2) explain database integrity;
(3) practice disposition of classified info;
(4) perform disposition of media and data;
(5) perform electronic records management;
(6) practice emergency destruction; and
(7) identify storage media protection and control procedures.

7. PLATFORM SPECIFIC SECURITY FEATURES/PROCEDURES

To be determined by agency/service/organization ISSO.

ANNEX B

REFERENCES

The following references pertain to this Instruction:

a. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, dated 16 November 1992

b. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated June 5, 1992

c. DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985

d. C.F.R. 32 Section 2003, National Security Information - Standard Forms, dated March 30, 1987

ANNEX C

BIBLIOGRAPHY

1. P.L. 100-235, Computer Security Act of 1987, dated January 8, 1988

2. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990

3. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, dated February 8, 1996

4. Office of Personnel Management, 5 CFR Part 930, Training Requirements for the Computer Security Act, dated January 3, 1992

5. National Computer Security Center TG-005, Trusted Network Interpretation (TNI), dated July 31, 1987